Designing Secure Protocols for Wireless Sensor Networks

A. Selcuk Uluagac[1], Christopher P. Lee[1], Raheem A. Beyah[2], and John A. Copeland[1]

[1] Communications Systems Center, School of Electrical and Computer Engineering
Georgia Institute of Tehnology, Atlanta, Georgia 30332, USA
[2] Communications Assurance and Performance Group, Georgia State University
34 Peachtree Street, Atlanta, Georgia 30303, USA
{selcuk,chris,jcopeland}@ece.gatech.edu rbeyah@cs.gsu.edu

Abstract. Over the years, a myriad of protocols have been proposed for resource-limited Wireless Sensor Networks (WSNs). Similarly, security research for WSNs has also evolved over the years. Although fundamental notions of WSN research are well established, optimization of the limited resources has motivated new research directions in the field. In this paper, we seek to present general principles to aid in the design of secure WSN protocols. Therefore, building upon both the established and the new concepts, envisioned applications, and the experience garnered from the WSNs research, we first review the desired security services (i.e., confidentiality, authentication, integrity, access control, availability, and nonrepudiation) from WSNs perspective. Then, we question which services would be necessary for resource-constrained WSNs and when it would be most reasonable to implement them for a WSN application.

Key words: Wireless Sensor Networks, Security in Wireless Sensor Networks, Security Services for Wireless Sensor Networks.

1 Introduction

Throughout the last decade, the introduction of WSNs to the networking field has gathered the attention of academia and industry. Today, WSNs are no longer a nascent technology and future advances in technology will bring more sensor applications into our daily lives as well as into many diverse and challenging application scenarios. For example, WSNs would be very instrumental in applications from real-time target tracking, homeland security, battlefield surveillance, surveillance of territorial waters, to biological and chemical attack detection [1].

In this regard, designing secure protocols for wireless sensor networks is vital. However, designing secure protocols for WSNs requires first the detailed understanding of the WSN technology and its relevant security aspects. Compared to other wireless networking technologies, WSNs have unique characteristics that need to be taken into account when building protocols. Among many factors, the available resources (i.e., power, computational capacities, and memory) onboard

the sensor nodes are severely limited. For instance, a typical sensor [2] operates at the frequency of 2.4 GHz, has a data rate of 250Kbps, 128KB of program flash memory, 512KB of memory for measurements, transmit powers between 100μW and 1mW, and 30m to 100m of communications range. Thus, the most important design parameter for WSN protocols is to be energy efficient. This fundamental fact heavily influences protocols that are designed for the WSN.

Although, over the years, a myriad of protocols have been proposed for WSNs and fundamental notions have been established well, trying to be energy efficient and optimize the limited resources available in WSN protocols have further brought new notions and directions in the WSN research. Some of these notions are directly in contrast to what have been considered and studied as reasonable for other types of wireless networks. For instance, today, it is believed that not all the communication layers from the protocol stack are needed to be implemented in the sensors [3]. This is reasonable as it both saves space from the implementation and reduces complexity. Thus, this work constitutes a bridge between salient features of the WSN protocols, applications and their security aspects by addressing the desired security services for WSNs.

The main goal of this work is to provide a basin of concepts for protocol designers to consider before attempting to build secure WSN protocols. Specifically, building upon the established concepts and the experience garnered from the previous research efforts in the literature, we sift through all the security services (confidentiality, authentication, integrity, access control, availability, and nonrepudiation). First, what a particular security service means from the WSN's perspective is discussed. Second, how that service has been studied in the literature is briefly addressed. Finally, we present further suggestions by questioning the need of that service for WSNs. We believe further improvements can be accomplished by unbundling some of the unnecassray security services, which may be contrary to most of the established principles.

The paper proceeds as follows. Sections 2 briely gives the communication and the threat models for WSNs. In threat models, we also introduce a new threat model, called Target-Based attacks as a complementary threat model to the current literature. Desired security services are explored in Section 3. Section 4 discusses which service should be provided for a particular scenario. Finally, section 5 concludes the paper.

2 The WSN Communication & Threat Models

In this section, we articulate the communication and the threat models for the WSN, which is significant to capture the security aspect of the problem. In WSNs, only sensor-to-sensor, sink-to-sensor, and sensor-to-sink communications can occur. In rare applications, where more than one sink is present, there may be a sink-to-sink communication as well. The possible communications are illustrated in Figure 1.

There are several threats to a WSN protocol. Conceptually, the threats could be listed from different perspectives. The previous research have listed threats

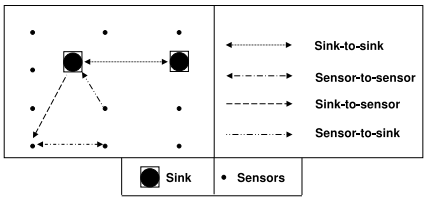

Fig. 1. WSNs communication model

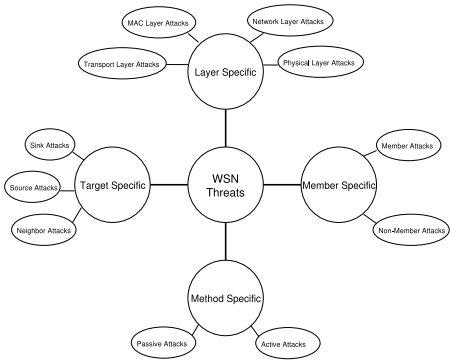

Fig. 2. WSNs threat model including the new Target-Based Attacks

according to how attacks are accomplished (e.g., Passive-Active Attacks)[4], on which layer of the communication stack they are realized (e.g., Layered Attacks) [5], and finally whether the malicious node becomes a member of the network during the attack or not (e.g., Member and Non-Member Attacks) [6]. Essentially, current literature for threat models resemble the ones done for wireless networks in general, which is a legitimate starting point, because many of the attacks could be borrowed from the literature for wireless networks. However, given the unique nature of a WSN, threats can be studied from another perspective. For instance, different functionalities could have been implemented at different parts of the network in order to efficiently utilize the resources of the WSN. Thus, an attacker first identifies where the critical functionalities are implemented in the network and then perpetrates its malicious intent on those identified targets. Thus, motivated to define another proper threat model for WSNs, in this paper, we also introduce a new threat model, *Target-Based Threat Model*, which is distinguished according to where and on which networking components the attacks are targeted (i.e., Sink, Neighbor, and Source Attacks). Target-based model complements the previous research on the issue. In reality, there is no hard line between these attacking types. The threat model for the WSN is given in Figure 2.

3 Desired Security Services from the WSNs Perspective

Structured definition of desired security services and mechanisms for the interconnection of open systems have been developed as an international standard by the International Telecommunication Union (ITU) inside Recommendation X.800 [7], which is referred to as the Security Architecture for OSI. This security architecture has been a valuable guideline for many researchers and practitioners who aim to develop secure systems. Thus, in this section we look at this reference security architecture from the perspective of WSNs.

Inside X.800, there are five major service categories: *Authentication, Access Control, Data Confidentiality, Data Integrity*, and *Nonrepudiation*. Although *Availability* has not originally been considered as one of the security services in X.800, it is also included in our discussion below, as it pertains to desired security services for WSNs.

Similar to other WSNs protocols and applications, three performance metrics are pertinent when providing security services for WSNs. These performance metrics are independent of the chosen encyption mechanism. One is the *storage*, another is the *communication*, and the last is *computational* cost. For WSNs, the *communication cost* is the costliest among all the others and the chosen security mechanism implemented should try to use these scare resources efficiently.

These security services are studied below. Specifically, first, what the particular security service means in the WSN's domain is given; second, how that service has been addressed in the literature is articulated briefly.

3.1 Confidentiality

WSN Perspective Definition: Confidentiality refers to the protection of the exchanged content (e.g., gathered data, reports, commands) among the sink(s) and the sensors. An adversary which has the privilege to access the content, should not be able to decode the exchanged messages in the network.

Current Approaches: Providing a confidential service to WSN applications requires the usage of cryptographic measures like encryption techniques. In general, two distinct forms of encryption approaches are in common use: *symmetric* and *asymmetric* key based schemes. Symmetric key based encryption uses the same key at both ends of the communication to encrypt and decrypt the information from ciphertext to plaintext and vice verse. On the other hand, with asymmetric key based encryption, a different key (one private and one public) are utilized to convert and recover the information.

The general important observation about encryption mechanisms is that one cannot claim that one encryption method is superior to another as it is essentially a matter of the key size and the computational effort in breaking the encryption algorithm [4]. The second aspect to confidentiality research in WSNs entails designing efficient *key management* schemes because regardless of the encryption mechanism chosen for WSNs, the keys must be made available to the communicating nodes (e.g., sources, sink(s)) to maintain the privacy of the channels. The key management process involves two fundamental steps: generation (after an analysis) and distribution of keys; and it is triggered by keying events (e.g., due to node addition or an attack) in the network. Nonetheless, it is not an easy task and even in some applications it may be daunting operation to visit a large number of sensors and update their keys (e.g., for underwater sensor applications). Thus, intelligent key management schemes are necessary for WSN.

There are two further observations for confidentiality research in WSNs. First, the research mainly focuses on different keying mechanisms rather than

on building efficient symmetric or asymmetric encryption algorithms. This is reasonable because it is not easy to devise a new encryption technique due to its complex and rigorous mathematical processes involved. Second, as for the keying mechanisms, it is seen that current research mainly revolves around the key distribution step because for the resource limited WSN, it is not efficient to repeat the analysis and key generation with every occurrence of a keying event.

The following list gives an overview of the research for both the encryption and key management mechanisms for WSNs.

- *Encryption mechanisms*: In recent works, the feasibility of two encryption techniques have been well scrutinized and understood for the WSN domain. With the current technological advances in the field of micro-electro-mechanical systems, symmetric encryption techniques is more tailored to WSNs. There are several reasons for this. First of all, using the same key at both ends saves the storage space. For instance in a simple worst case scenario assume that there are N number of nodes in the network. While for symmetric encryption, a given node must posses N-1 number of keys in order to communicate to the other N-1 nodes, for asymmetric encryption, the same node must have N keys, N-1 for others' public keys, one for its own private key. Considering the fact that the key sizes for symmetric algorithms (e.g., 128 bits for AES) are generally smaller than those of asymmetric ones (e.g., recommended 1024 bits for RSA and 160 bits for Elliptic Curve Cryptography (ECC) Based Public Key Scheme), one can conclude that depending on the specified key size of the particular algotrithm chosen, the symmetric encryption algorithms may help save from the per-node storage space. Secondly, the symmetric encryption algorithms have been known to utilize the resources more efficiently than their asymmetric counterparts as their cryptographic operations take lesser time and require much less energy consumption than that of asymmetric cryptographic ones [8]. This is primarily due to the fact that the symmetric encryption algorithms are faster in computation as they employ more primitive operations in their algorithms like substitution and permutation of symbols, which are implemented at the hardware level via shifts and XORs, rather than operations applying mathematical functions like modular arithmetic and exponentiation, which are the basis of public key encryption mechanisms. Lastly, the exchange of smaller size keys, when needed in a WSN application, consumes less communication resources, which favors symmetric schemes. A detailed discussion of key mechanisms are given below.
- *Key management mechanisms*: As mentioned above, there are two fundamental steps in the key management process: *generation* and *distribution* of keys. The *key generation* step deals with generation of the keys. Depending on the key type that is going to be deployed in the WSN, the keys can be generated once or multiple times during the lifetime of the WSN. The practical approach adopted so far in this avenue of research has been to generate one time different keys such as session, network-wise, master, and group-wise keys depending on the topology and on the application requirements

of WSNs. While this helps decrease the computation cost for WSNs, it may increase the storage over nodes depending on the key distribution scheme. The second step is the *distribution* of keys. The keys should be made available to the nodes without allowing others to see the keys. Traditionally, the keys have been exchanged between the end-points of the communication directly, or indirectly through trusted intermediaries (e.g., Key Distribution Center). The keys could be distributed to the sensors before the network is deployed or they could be re-distributed to nodes on demand as triggered by keying events. In the jargon of security research for WSNs, the former is phrased as *Static Key* management whereas the latter is as *Dynamic Key* management. For WSNs, the communication cost dominates other critical cost parameters, i.e., storage and computation [9]. Thus, the research for key distribution has focused more on static key management schemes. *Static key* management schemes perform key management functions statically prior to or shortly after network deployment. One famous pioneering work in this avenue is by Eschenauer and Gligor [9] [8], where each sensor in the WSN is pre-configured with a random subset of keys from a large key pool. To agree on a key for communication, two sensor nodes find one common key within their subsets and use this key as their shared secret key. On the other hand, *dynamic key* management schemes perform the key management steps either periodically or on demand due to keying events in the network. The leading approach in dynamic keying schemes involves exclusion-based systems [10], the basic notion of which requires each node to have k keys out of $k + m$ keys. m keys are disguised from the attackers and are used only when new keys need to be created once keying events are triggered in the network.

3.2 Authentication

WSN Perspective Definition: Authentication service involves genuineness of the communication. An authentication mechanism verifies if the exchanged information is emanating from the legitimate participant of the WSN because a malicious entity (e.g., a compromised node) may be able to inject counterfeit content or resend the same content into the network. Moreover, the X.800 specification recommends two sub-cases for authentication. The first involves the authentication of the peer entity and the second deals with the authentication of the origin of the data. For WSNs, the former means authentication of all the nodes that participate in the communication. Authentication can be done between two nodes communicating or one node (e.g., cluster head) and several other nodes around that node (i.e, broadcast authentication). The latter can be implemented at the sink or at an intermediary sensor node where data aggregation takes place.

Current Approaches: There are several traditional methods of authentication in the literature [4]. One is password based method depending on the premise of showing that one knows a secret. The node sends a password with its login

information. The receiver verifies that the node is legitimate node by checking that the password is associated with the sender node.

The other one is cryptographic-based method, which is also called challenge-response. A classic technique to provide authentication would be to utilize Message Authentication Codes (MAC). The authenticated sensor node is required to provide the MAC code to be authenticated by the the authenticator sensor node. For MACs, hashes, symmetric key-based encryption, asymmetric key-based encryption methods may all be utilized. Thus, there are several practical ways of creating MACs, but simply creating a MAC involves possesing the same secret at both ends and either encrypting the hash of the content with that key or hashing both the key and the content together. However, as discussed in the confidentiality subsection above, the encryption mechanisms have their associated costs, thus they should be employed with caution.

The last authentication method is address-based or identy-based. For this, the authenticator sensor node can check the identity or the location of the sender node. The passwords is not sent across the network with these schemes. In comparison to the previous two mechanism, this method would be very practical for WSNs but would not provide a strong authentication mechanism because it is trivial to spoof a sensor ID.

Two of the former leading works include SPINS [11] and TinySec [12]. They both employ symmetric encryption algorithms and work at the link layer.

3.3 Integrity

WSN Perspective Definition: The recipients in the WSN should be able to detect if the exchanged content between the communicating participants of the WSN have been altered. Furthermore, for the WSN, the integrity service should also ensure that the exchanged content is not deleted, replication of old data, counterfeit, or stale.

Current Approaches: Integrity of the exchanged content is usually provided with the digest of the content appended to the content itself. When the recipient sensor node receives the message it checks to see if the digest of the content that it computes and the digest received equals each other. If they are, then it accepts it as a legitimate message.

Content digests in integrity are created with the usage of hashing algorithms. There are many hashing algorithms in use today. Usually, hashing algorithms do not require the presence of keys unless they are specifically designed to work with keys like keyed-hashing (e.g., HMAC, CMAC). Thus, their impact on a sensor node is only confined with their computational efficiencies. However, as for the keyed-hashing algorithms, previously discussed issues emanating from key generation, key storage, and key exchange are also pertinent here, hence the keyed-hashing techniques must utilize the resources (computation, communication, and storage) efficiently

Staleness of the data is of utmost significance in the integrity checking because decision processes of some applications may especially depend on if the

data is recent or not. For example, in one very specific WSN application, a certain territory (e.g., territorial waters) could be protected with mines that are detonated by sinks. The freshness and the correct timing of the messages from the sensor nodes in this type of application is very important. A simple solution for these types of applications would be to use counters for the exchanged content. Lastly, another desired aspect of the integrity service may involve providing a recovery mechanism from the altered content.

3.4 Access Control

WSN Perspective Definition: With access control, unauthorized use of a resource is prevented in WSNs. It addresses which participant of the network reaches which content or service. For instance, sensor nodes should not be allowed to have the privileges of sinks such as changing network-wide parameters of the WSN protocols. Thus, limiting services or functionalities depending on the participant would be appropriate.

Current Approaches: One of the most challenging security services for WSNs is access control; hence, this is perhaps why access control for WSNs is one of the security services that have not been studied well in the literature [13]. We believe that part of this is because it is hard to formulate an access control scenario for WSNs. In practical implementations, normally there is one terminating point (i.e., sink) in the network where all the data collected from the network is collected. Thus, other sensors are not expected to access to any resource that may be hosted by other nodes. This is a reasonable expectation for WSN applications where sensors send their readings based on an event. However, there may be sensor applications where source sensor nodes are queried by other sensor nodes as well. For these circumstances, the access control policies can be used. An access control policy should prevent unauthorized nodes from accessing the important information.

Setting access policies may also be practical and instrumental for cluster-based or hierarchical sensor node implementations.

3.5 Nonrepudiation

WSN Perspective Definition: Nonrepudiation is service of ensuring that a sensor can not refute the reception of a message from the other involving party or the sent of a message to the other involving party in the communication. According to the X.800 recommendation, the former is the destination and the latter one is called the origin nonrepudiation.

Current Approaches: Similar to access control, nonrepudiation has not been formulated well int the WSNs domain. This could be attributed to the lack of need of such a service for WSNs. Or, it could have been thought inside integrity or authentication services implicitly.

Although the need for nonrepudiation service may not seem to be obvious, we think that it is an achievable important service to contemplate and that there are some practical advantageous in providing this service. A digital signature scheme (DSS) [4], which is based on utilizing encryption methods would also address nonrepudiation. Symmetric and asymmetric encryptions can be utilized for DSS. However, their viabilities should be explored in more detail for WSNs. For instance, on the one hand, using the same key both for signature and verification may be vulnerable to another sensor's impersonation of the original sensor's signature. On the other hand, however, employing asymmetric encryption based algorithms may be costly. Naturally, providing nonrepudiation service may facilitate the endorsement or proof by another entity for a sent or receipt message in WSN. Thus, alternatively, some other trusted node, either the sink or an aggregator node, in the network could provide this service.

3.6 Availability

WSN Perspective Definition: Due to threats to the WSN, some portion of the network or some of the functionalities or services provided by the network could be damaged and unavailable to the participants of the network. For instance, some sensors could die earlier than their expected lifetimes. Thus, availability service ensures that the necessary functionalities or the services provided by the WSN are always carried out, even in the case of attacks.

Current Approaches: Availability is a security service that has not been originally considered as one of the security services inside the X.800 recommendation. It may be claimed that it is independent of the security services. The outcome of the secure services provided by the network should guarantee the operations and functionalities aimed by the WSN application. Availability service for WSNs have been mostly studied from the perspective of Denial-of-Service type attacks [14] in the literature. One other pertinent study regarding availability has focused on the connectivity properties of WSNs [15].

4 When to Employ Specific Security Services

Sensor nodes are severely limited in their capabilities. There are three important design parameters for WSNs: communication, computation, and storage cost. The cost of communication dominates over those of the computation and storage. So, any security service designed for WSNs should always try to minimize the cost of these parameters. Thus, providing a security service comes with its associated costs naturally as it is an additional service on top of whatever is provided by the network.

When we look at the security services in general, we see that they are often provided as bundled services. Another observation from the literature is that in comparison to other security services, confidentiality has been explored more

because it is fundamental to all of the other security services, except for availability. We believe that for resource constrained devices like sensor nodes in WSNs, there can be further minimization of the associated cost by just unbundling the unnecessary services. This would require the understanding of the needs of the network. Therefore, security services should be tailored to the applications, as it would be a waste of important resources in the network if all the security services are unnecessarily implemented. Looking at the security services and the improvements in the field, below is a discussion of how the security services should be analyzed for WSNs.

- Confidentiality of data should be always be questioned as the confidentiality will always be the most costly security service among all the security services. Unless it is utmost necessary for the WSN, it may not be employed. Integrity check on the data may suffice to determine the activity of a malicious entity in the WSN. Thus, confidentiality can be unbundled from the rest of the services and provided as an additional security service for the WSN and be addressed separately from the other services.
- Authentication service can be considered as a prevention mechanism for WSNs applications. This is reasonable because when authenticating a untrusted sensor node, if that node is malicious one, it may have or not perpetrated its malicious intent yet. With authentication, the malicious node may be blocked from its activity. Thus, authentication may be used as a prevention mechanism. Furthermore, authentication may be necessary for aggregator sensor nodes, which collect the sensors' readings, where the agregator sensor nodes asks the source sensor nodes for their sensor readings. The source nodes may need to authenticate the aggregator node.
- Providing integrity definitely determines if a malicious activity exists in the network or not. It can be considered as a detection mechanism rather than a prevention mechanism like authentication. Specifically, integrity check for WSNs can be done either at every sensor node or at data-aggregating nodes or sink(s). Checking at every node increases the computation cost, but eliminates the fake data immediately and prevents that data from propagating further. On the other hand, checking the integrity at aggregator nodes or sinks save from the computation, but not from the communication cost. This is an application specific parameter that should be considered when providing integrity for WSNs, which is a topic for further investigation.
- Intelligent bundling of the services is possible. For instance, the integrity can be embedded inside an authentication service. The nice thing about asymmetric systems is that they can be used for both authentication and integrity purposes. It is even possible to use an asymmetric encryption algorithm to provide authentication, integrity, and nonrepudiation. Although asymmetric encryption mechanisms are costlier than symmetric encryption mechanisms, further security services can be addressed in an all-in-one fashion. However, their applicability for WSNs needs further investigation.
- Access control comes naturally after authentication; thus, it may be beneficial to bundle these two. However, confidentiality and access control are separate issues that can be de-coupled and addressed separately.

- It is always cost effective for WSNs to employ security algorithms with smaller key sizes. Smaller key sizes will help save from the network storage, and further, if the keys are exchanged in the network, it will save from the communication as well because communication of smaller keys consumes less communication overhead. Moreover, when smaller keys and asymmetric encryption is necessary, ECC based algorithms should be favored over the others as ECC based ones, have much better efficient utilization of the resources in place of others (e.g., RSA)
- Usage of different keys such as session, network-wise, master, and group-wise keys should be considered to isolate and to futher help counter malicious activities. Furthemore, albeit costlier than the static key management schemes, dynamic key management schemes is more tailored to WSN applications. There may be ways to generate keys dynamically without too much overhead. For instance, depending on something unique that a sensor posses, keys can be generated instead of being exchanged. For instance, the residual batter life or energy on a node [16] or identity of the node could be utilized for this. However, depending on the application type and the needs, if the lifetime of the network is more important than security, then static key management schemes may be preferred in place of dynamic.
- Due to the resource constrainted nature of WSNs, there have been new ideas that are shaping the future of WSNs. Some of the promising ones include collaboration of sensor for the distributed networking functionalities, and de-layered of TCP/IP stack. There would be further savings from the scarce resources of WSNs, if these are considered when building secure WSN protocols. For instance, collaborative security, application-oriented security, and non-layered security approaches may be promising but they need further investigation.
- Availability should not be considered outside of security services, the network should have worst case secure data delivery scenarios in case of any security breach or malicious attack. However, this can be thought in a layered fashion. Unless there is a security problem in the network, the alternative availability mechanism may not be considered. However, this is again an application oriented issue for WSNs. For some applications, where the timely collection of data is utmost important, the availability should be considered at the same as security services.
- For application where different types of sensor nodes co-exist or a composite of events [17] occur in the same WSN application, it may be very important to provide an access control service. Similarly, having access policies may be instrumental for cluster-based or hierarchical sensor node implementations.

5 Conclusion

Both WSNs and the security for WSNs research fields have matured over the years. Furthermore, optimization of the limited resources has motivated new research directions in the field. In this work, considering the established concepts

and new directions, we have discussed general principles for researchers who seek to design secure WSN protocols. Specifically, we have reviewed the desired security services, i.e., confidentiality, authentication, integrity, access control, availability, and nonrepudiation, and their necessity from the WSN perspective. We have determined and listed several valuable suggestions for protocols builders. The protocol designers should determine what is best for their WSN applications and needs.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks (Elsevier) Journal*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] Xbow, "Crossbow technology," 2008. [Online]. Available: http://www.xbow.com/

[3] I. F. Akyildiz, M. C. Vuran, and O. B. Akan, "A cross layer protocol for wireless sensor networks," in *Proc. CISS '06*, Princeton, NJ, March 2006.

[4] W. Stallings, *Cryptography and Network Security: Principles and Practices (3rd edition)*. Prentice Hall, 2003.

[5] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of security attacks in sensor networks," in *The First IEEE International Conference on System Integration and Reliability Improvements*, Hanoi, Vietnam, Dec 2006.

[6] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38– 43, December 2004.

[7] I.-T. R. X.800, "Security architecture for open systems interconnection for ccitt applications," 1991.

[8] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the ACM CCS '02*, 2002, pp. 41–47.

[9] Y. W. Law, J. Doumen, and P. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, no. 1, pp. 65–93, 2006.

[10] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, April 2006.

[11] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," *Wireles Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[12] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *ACM SenSys 2004*, November 2004.

[13] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," *Elsevier's AdHoc Networks Journal*, vol. 5, no. 1, pp. 3–13, January 2007.

[14] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[15] R. D. Pietro, L. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "How to design connected sensor networks that are provably secure," *Securecomm*, pp. 89–100, 2006.

[16] H. Hou, C. Corbett, Y. Li, , and R. Beyah, "Dynamic energy-based encoding and filtering in sensor networks," in *Proc. of the IEEE MILCOM*, October 2007.

[17] C. Vu, R. Beyah, and Y. Li, "A composite event detection in wireless sensor networks," in *Proc. of the IEEE IPCCC*, April 2007.